SECURITY AND APPLICATIONS ADMINISTRATOR

GRADE: 24 **FLSA: EXEMPT**

CHARACTERISTICS OF CLASS:

The Security and Applications Administrator performs difficult professional and administrative work ensuring that the City's computer systems are protected and secure. Additionally, this position supports several applications, including database applications used by various departments. Responsibilities include establishing and enforcing security policies, reviewing and auditing the City's firewall rules, routinely reviewing the City's virus and spam filtering capabilities, and intrusion detection systems. Periodic security audits will be performed and access controls will be reviewed on a regular basis. The work includes handling most assignments with independence under general management direction. The work can require moderate physical effort. This is a highly sensitive position and can involve stressful and complex situations.

EXPECTATIONS OF ALL CITY EMPLOYEES:

- Learn and demonstrate an understanding of City, department, division and team goals.
- Serve and meet the needs of customers during routine or emergency situations.
- Ability and willingness to work as part of a team, to demonstrate team skills and to perform a fair share of team responsibilities.
- Ability to assess his/her work performance or the work performance of the team.
- Plan and organize his/her work, time and resources, and if applicable that of subordinates.
- Contribute to the development of others and/or the working unit or overall organization.
- Produce desired work outcomes including quality, quantity and timeliness.
- Communicate effectively with peers, supervisors, subordinates and people to whom service is provided.
- Understand and value differences in employees and value input from others.
- Consistently report to work and work assignments prepared and on schedule.
- Consistently display a positive behavior with regard to work, willingly accept constructive criticism and be respectful of others.

EXAMPLES OF DUTIES:

- Serves as the primary computer security expert for the City.

- Establishes security policies and ensures they are followed by employees based on government/industry-standard best practices for LAN/WAN and wireless networks.
- Performs routine audits of various systems and analyzes access controls for vulnerability.
- Conducts user audits where required.
- Routinely reviews the City's firewall rules and policies to protect the City's IT assets.
- Installs and configures intrusion detection systems and other security measures to anticipate and thwart security threats.
- Periodically reviews the City's virus protection and spam filters systems to ensure they are working effectively.
- Manages and ensures the security of databases and data transferred both internally and externally.
- Audits and reviews server logs, firewall logs, intrusion detection logs, and network traffic for unusual or suspicious activity and takes corrective action where necessary.
- Manages review of physical security and access logs of the City's data center, server rooms, switch rooms and other sensitive IT facilities.
- Designs, implements and maintains disaster recovery procedures.
- Designs, performs and oversees penetration testing of all systems in order to identify and resolve vulnerabilities.
- Recommends, schedules (where appropriate) and applies fixes, security patches, disaster recovery procedures, and any other measures required in the event of a security breach.
- Keeps current on emergency security alerts and issues.
- Supports a variety of applications including: ROAM Secure R-911, Crimestar, Route Manager, redlight, speed camera, LINX and other systems as directed.
- Performs other duties as required.

QUALIFICATIONS:

Required Training and Experience:

A Bachelor's degree from an accredited university or college with significant coursework in information security, computer science or other related field and four years of experience working in an information security role. Hands on experience with devices such as hubs switches, and routers and experience conducting security audits. Additional education may be substituted for up to two years of the work experience. Possession of a driver's license valid in the State of Maryland.

Preferred Knowledge, Skills and Abilities:

- Extensive knowledge of information and computer security. Certification in either CISSP (Certified Information System Security Professional), or SSCP (Systems Security Certified Practitioner).

- Hand-on knowledge of firewalls, intrusion detection systems, anti-virus software, and other industry-standard techniques and practices.
- Strong knowledge of TCP/IP and network administration/protocols.
- Knowledge of applicable practices and laws relating to data privacy.
- Knowledge and training in supporting Microsoft SQL server databases.
- Knowledge of operating systems including: Linux, Windows Server 2000, and 2003.
- Knowledge of Cisco IOS and Cisco Firewalls.
- Strong organizational skills.
- Strong interpersonal and oral communications skills.
- High level of analytical and problem-solving abilities.
- Ability to conduct research into security issues and products as required.
- Ability to proactively detect threats and take corrective actions.
- Ability to develop and enforce security policies.
- Ability to understand and background in conducting penetration testing.
- Ability to create, maintain and test recovery plans.
- Ability to effectively prioritize and execute tasks in a high-pressure environment.
- Ability to lift and transport moderately heavy objects, such as servers and peripherals.
- Ability to conduct risk assessments.